Pearson BTEC Level 3 Nationals Diploma, Extended Diploma

Information Technology

Unit 11: Cyber Security and Incident Management

Part A

Sample assessment material for first teaching September 2017
Supervised hours: 5 hours

Paper Reference
20158K

You will need:
Risk_Assessment.rtf
Security_Plan.rtf

Instructions

- **Part A** and **Part B** contain material for the completion of the set tasks under supervised conditions.
- There are 43 marks for **Part A** and 37 marks for **Part B**, giving a total mark for the set task of 80.
- **Part A** and **Part B** are specific to each series and this material must be issued only to learners who have been entered to take the tasks in the specified series.
- This booklet should be kept securely until the start of the 5-hour, **Part A** supervised assessment period.
- **Part A** will need to have been completed and kept securely before starting **Part B**.
- Both parts will need to be completed during the 3-week period timetabled by Pearson.
- **Part A** and **Part B** tasks must be submitted together for each learner.
- This booklet should not be returned to Pearson.
- Answer **all** activities.

Information

- The total mark for this paper is 43.

Turn over ▶

S54092A

1/1/1/1/1/1/1/1/1

S 5 4 0 9 2 A

Pearson

Instructions to Teachers/Tutors and/or Invigilators

This paper must be read in conjunction with the unit information in the specification and the *BTEC Nationals Instructions for Conducting External Assessments (ICEA)* document. See the Pearson website for details.

Refer carefully to the instructions in this task booklet and the *Instructions for Conducting External Assessments (ICEA)* document to ensure that the assessment is supervised correctly.

Part A and **Part B** set tasks should be completed during the period of three weeks timetabled by Pearson. **Part A** must be completed before starting **Part B**.

The 5-hour, **Part A** set task must be carried out under supervised conditions.

The set task can be undertaken in more than one supervised session.

Electronic templates for activities 1 and 2 are available on the website for centres to download for candidate use.

Learners must complete this task on a computer using the templates provided and appropriate software. All work must be saved as PDF documents for submission.

Teachers/tutors may clarify the wording that appears in this task but cannot provide any guidance in completion of the task.

Teachers/tutors and invigilators should note that they are responsible for maintaining security and for reporting issues to Pearson.

Maintaining Security

- Learners must not bring anything into the supervised environment or take anything out.
- Centres are responsible for putting in place appropriate checks to ensure that only permitted material is introduced into the supervised environment.
- Internet access is not permitted.
- Learner's work must be regularly backed up. Learners should save their work to their folder using the naming instructions indicated in each activity.
- During any permitted break, and at the end of the session, materials must be kept securely and no items removed from the supervised environment.
- Learners can only access their work under supervision.
- User areas must only be accessible to the individual learners and to named members of staff.
- Any materials being used by learners must be collected in at the end of each session, stored securely and handed back at the beginning of the next session.
- Following completion of **Part A** of the set task, all materials must be retained securely for submission to Pearson.
- **Part A** materials must not be accessed during the completion of **Part B**.

Outcomes for Submission

Each learner must create a folder to submit their work. Each folder should be named according to the following naming convention:

[Centre #]_[Registration number #]_[surname]_[first letter of first name] _U11A

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345_F180542_Smith_J _U11A

Each learner will need to submit 3 PDF documents, within their folder, using the file names listed.

Activity 1: activity1_riskassessment_[Registration number #]_[surname]_[first letter of first name]

Activity 2: activity2_securityplan_[Registration number #]_[surname]_[first letter of first name]

Activity 3: activity3_managementreport_[Registration number #]_[surname]_[first letter of first name]

An authentication sheet must be completed by each learner and submitted with the final outcomes.

Instructions for Learners

Read the set task information carefully.

Plan your time carefully to allow for the preparation and completion of all the activities.

Your centre will advise you of the timing for the supervised period. It is likely that you will be given more than one timetabled session to complete these tasks.

Internet access is not allowed.

You will complete this set task under supervision and your work will be kept securely at all times.

You must work independently throughout the supervised assessment period and must not share your work with other learners.

Your teacher/tutor may clarify the wording that appears in this task but cannot provide any guidance in completion of the task.

You should only consider threats, vulnerabilities, risks and security protection measures that are implied and/or specified in the set task brief.

Part A materials must not be accessed during the completion of **Part B**.

Outcomes for Submission

You must create a folder to submit your work. Each folder should be named according to the following naming convention:

[Centre #]_[Registration number #]_[surname]_[first letter of first name] _U11A

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345_F180542_Smith_J _U11A

You will need to submit 3 PDF documents, within your folder, using the file names listed.

Activity 1: activity1_riskassessment_[Registration number #]_[surname]_[first letter of first name]

Activity 2: activity2_securityplan_[Registration number #]_[surname]_[first letter of first name]

Activity 3: activity3_managementreport_[Registration number #]_[surname]_[first letter of first name]

You must complete an authentication sheet before you hand your work into your teacher/tutor.

Set Task Brief

Bankside College

Bankside College has 800 pupils, aged from 11 to 18. Built in 1876, the college building has been extended over the years with the addition of administrative offices and classrooms.

The Information Technology (IT) department has a server room, an office and classrooms in the main building. Some of the old network technology needs to be replaced.

The college governors have raised money to pay for the new network technology. A new technology block is being built and it should be completed before the start of the new academic year.

The IT department will share the new block with the Design and Technology (D&T) department. Both departments will get new IT provision and the IT provision will be improved for the rest of the college. The target is for every member of staff and every pupil to have an Android-based tablet.

The plan of the college, including the new Technology Block, is shown in **Figure 1**.

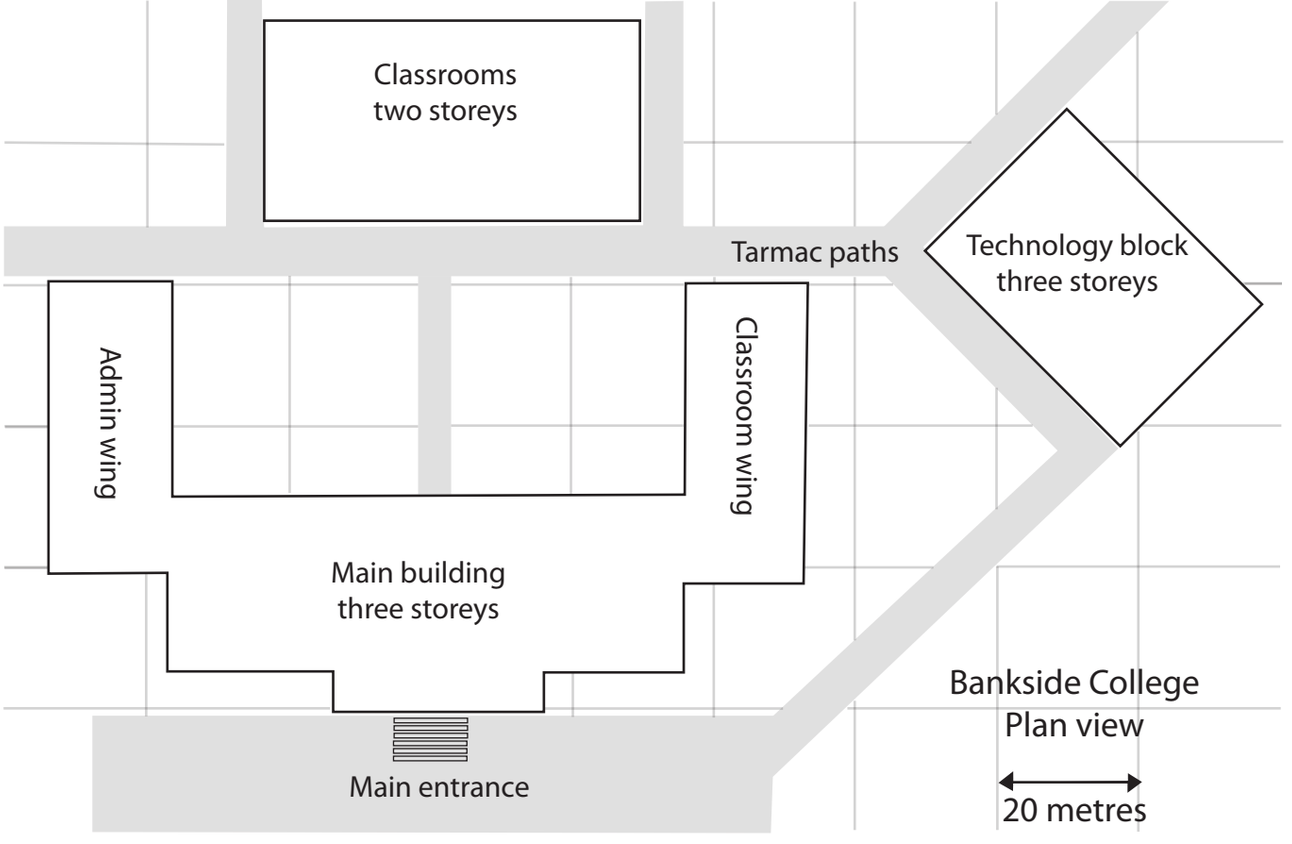

Figure 1

These problems have arisen.

The Head of IT has decided to retire and the governors want to appoint a replacement.

The Network Manager will take maternity leave at the end of the summer term. There are two highly skilled IT technicians who also look after the D&T equipment. Neither of them want to take on a managerial role.

The governors are under pressure to keep costs down so they have decided to reconsider the project. They have formed a Project Management Committee. The committee members are effective users of IT but have been chosen more for their commercial and management expertise rather than their technical knowledge.

Briefing on current system

The current Head of IT and the Network Manager have provided a briefing on the current system. You have been appointed as the Technical Adviser to the Project Management Committee. You will report to the committee and provide documents to inform and assist them in making their decisions.

The Bankside College Local Area Network (LAN) has two sub-domains, Teaching and Admin. These have their own domain controllers, running Server 2008. Both domain controllers are located in the IT department. Each sub-domain has a Network Attached Storage (NAS) device and several networked printers.

The Teaching sub-domain services the IT and D&T departments. It has 80 computers in the IT department, arranged in three classrooms. There are a further 10 computers in the D&T department. All the Teaching computers use Windows 8.1.

The Admin sub-domain contains all other college computers in Bankside College. These include those in the administration offices, the staffroom, staff offices and anywhere else where computers have been set up over the years. The Admin computers vary in make, age and capability. They currently use a mix of Windows 8.1, 7, Vista, and XP. They are replaced or added to when necessary.

Redevelopment plan

A meeting of the Project Management Committee agreed these points on the redevelopment of the Bankside College network.

1. The Admin sub-domain server and NAS device will be moved from the Main Building to the Admin wing.

2. The current internet access system will be retained. This consists of a fibre optic connection to an Internet Service Provider (ISP) supplied router, located in the Admin wing.

3. The Bankside College network must be protected against intrusion from the internet.

4. The Teaching sub-domain server and NAS device will be moved from the main building to the Technology Block.

5. The 80 computers in the old IT department will be replaced by new machines in the Technology Block; two classrooms of 25 plus five spares.

6. In other classrooms pupils will use Android-based tablets provided by the college. They will be rooted so that the college keeps admin control over the devices.

7. All teachers and administrators will have the same type of Android-based tablets as the pupils. Administrators will be restricted to the Admin sub-domain but teachers must be able to connect to both Teaching and Admin.

8. Pupils must not have access to the Admin sub-domain or to teachers' files on the Teaching sub-domain.

9. The best 20 of the existing computers will be reused in the D&T department for CAD/CAM work. The Head of D&T wants the computers to be movable, so that they can be used in any of the D&T rooms. Pupils will used Android-based tablets in all other D & T lessons.

10. Each floor in the Technology Block will have two new, networked, colour laser printers.

11. Each classroom in the Technology Block will have a WiFi-networked data projector.

12. The IT and D&T departmental offices will each have a computer.

Figure 2 shows the proposed layout. Mobile devices are not shown but need to be able to connect anywhere in the college.

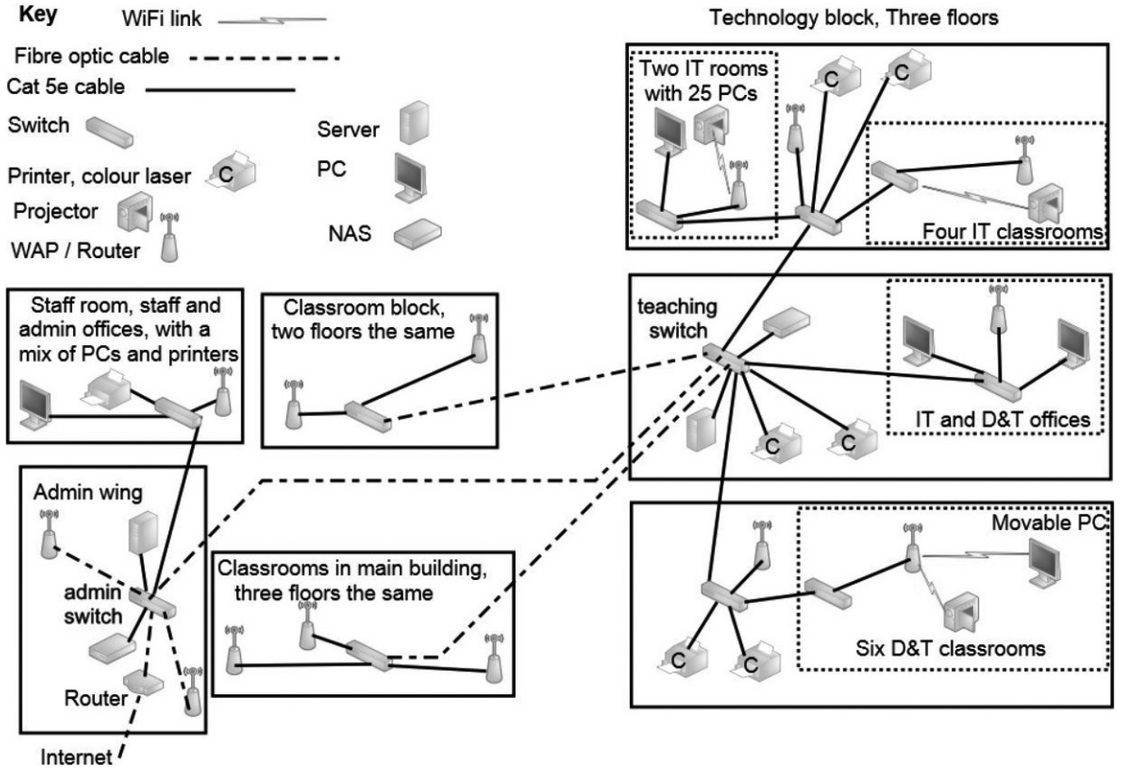

Figure 2

The governors are aware that having more devices in the network is likely to lead to increased security problems.

You have been hired to advise on cyber security. They would like to see your recommendations for securing the enlarged Bankside College network.

Part A Set Task

You must complete ALL activities in the set task.

Read the set task brief carefully before you begin and note that reading time is included in the overall assessment time.

You should only consider threats, vulnerabilities, risks and protection measures that are implied and/or specified in the set task brief.

Design cyber security protection measures for the given computer network.

Activity 1: Risk assessment of the networked system

Duplicate (copy and paste) and complete the risk assessment using the template given for each threat.

Produce a cyber security risk assessment using the template **Risk_Assessment.rtf**

Save your completed risk assessment as a PDF in your folder for submission as **activity1_riskassessment_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 1 hour and 30 minutes on this activity.

(Total for Activity 1 = 8 marks)

Activity 2: Cyber security plan for the networked system

Using the template **Security_Plan.rtf** produce a cyber security plan for the computer network using the results of the risk assessment.

For each protection measure, you must consider:

(a) threat(s) addressed by the protection measure
(b) action(s) to be taken
(c) reasons for the action(s)
(d) overview of constraints – technical and financial
(e) overview of legal responsibilities
(f) overview of usability of the system
(g) outline cost-benefits
(h) test plan.

Duplicate (copy and paste) and complete the cyber security plan using the template given for each protection measure, as appropriate.

Save your completed security plan as a PDF in your folder for submission as **activity2_securityplan _[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 2 hours and 30 minutes on this activity.

(Total for Activity 2 = 20 marks)

Activity 3: Management report justifying the solution

Produce a management report, justifying how the proposed cyber security plan will meet the security requirements of the set task brief.

The report should include:

- an assessment of the appropriateness of your protection measures
- a consideration of alternative protection measures that could be used
- a rationale for choosing your protection measures over the alternatives.

Save your completed management report as a PDF in your folder for submission as **activity3_managementreport_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 1 hour on this activity.

(Total for Activity 3 = 12 marks)

(TOTAL FOR TECHNICAL LANGUAGE IN PART A = 3 MARKS)
TOTAL FOR PART A = 43 MARKS